Journal of Theoretical and Applied Information Technology
20th May 2013. Vol. 51 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INTEGRITY OF DIGITALLY SIGNED MESSAGES USING JOINT SIGNATURE SCHEME

[1]SANIA HABIB, [2]DR. MALIK SIKANDAR HAYAT KHIYAL, [3]MUKHTIAR BANO AND, [4]AIHAB KHAN

[1,3]Department of Software Engineering, Fatima Jinnah Women University, The Mall, Rawalpindi, Pakistan.
[2]Head of Aacademic (ES), Army Public College Of Management Sciences, Khadim Hussain Road, Lalkurti, Rawalpindi, Pakistan.
[4]Department of computing, Iqra University, Islamabad, Pakistan.
E-mail: saniahabib2007@yahoo.com, m.sikandarhayat@yahoo.com, , banobrohi22@yahoo.com, aihabkhan@yahoo.com

ABSTRACT

In this era of advanced technology, mobile commerce is going to become popular due to rapid development of technology but this technology needs a lot of struggle for maintaining secure communication and protection from threats. In this research, a mechanism for secure and authentic communication in mobile commerce based on joint signature scheme is presented. This technique ensures the integrity of digitally signed messages using joint signature scheme which show that the message which is sent by the message sender have not been altered by any unauthorized person by digitally signing the message. This technique is efficient in mobile domain because it is less computative and easily used with limited resources in mobile commerce. Joint signature scheme is based on hash functions and encryption/decryption technique to produce joint signature with the help of message sender and trusted third party and also to authenticate the message for the message sender and the message receiver. This technique overcomes the drawbacks of traditional digital scheme, such as computation/communication load, complexity, public key operations etc.

Keywords: *M-Commerce, Joint Signature, Encryption, Cryptographic Hash Function, Password; Salt value, Message Integrity*

1. INTRODUCTION

Commerce is the exchange of goods or services between persons or companies. Now a day's commerce can be conducted through the internet and other computer networks. This electronic exchange of items is known as Electronic commerce or e-commerce. A large percentage of electronic commerce is conducted entirely electronically for virtual items such as access to premium content on a website, but most electronic commerce involves the transportation of physical items in some way.

Mobile commerce also known as next-generation e-commerce enables the users to perform the electronic commercial transactions wherever they go without needing to find a place to plug in. M-commerce allows the use of emerging technologies such as cell phones, personal digital assistants (PDA), Smart phone, Earpiece and other hand held devices that have operate with Internet access [1].

Security is the biggest issue in the field of m-commerce because without secure commercial information exchange and safe electronic financial transactions over mobile networks, no one will trust m-commerce. A joint-signature scheme can be used as one of the security primitives to address different security services. The scheme enables a mobile user to securely and efficiently instruct his/her network operator for m-payment related actions. It is based on the use of the one-way hash function and traditional digital signature method, but in a collaborative manner with the network operator. The joint-signature scheme achieves the same security services as those by a traditional digital signature scheme, i.e. message origin authentication, and non-repudiation of origin, but offers lower computational cost for the mobile user. In addition, it imposes lower communication cost in comparison with proxy/server-aided signature schemes. A notable advantage offered by this approach is that it does not require mobile users to store electronic money (e-money) on their mobile devices, which eliminates a range of security problems related to the

Journal of Theoretical and Applied Information Technology
20th May 2013. Vol. 51 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

storage, transmission and access to the e-money. Nor does it require the use and secure transmission of credit or debit card numbers over the air interface. In other words, this approach reduces the use of mobile phone resources and the security risks [2].

A. Contributions

Our contribution is to digitally sign the message with the help of Trusted Third Party to ensure that the message contents are authentic that is sent from Message Sender to Message Receiver.

2. RELATED WORK

Joint signature scheme is a new scheme and it is proposed by [1] in 2004 ACM Symposium on Applied Computing. This technique overcome the security issues related to m-commerce e.g. authentication, non-repudiation, confidentiality, integrity etc. But this technique was not implemented at that time, so we took this scheme as a base for the integrity of digitally signed message by the mobile user for purchasing goods online. Very few works is previously done for the integrity but techniques which have been used for the integrity have several drawbacks. Also these techniques were based on traditional digital signature scheme like [5] which has drawbacks in limited resources of mobile domain.

Server-aided technique proposed by [3] for the mobile commerce uses trusted proxy server to co-ordinate transactions between user and vendor. It is based on the [5] scheme and involves the one-time password mechanism to establish session key in advance between user and vendor with the help of trusted proxy server. This technique is divided into two phases; negotiation phase and authentication phase. This technique discussed different aspects of security issues like anonymity etc but with the drawback of high communication load as because it involves negotiation as well as authentication phase in communication between mobile user and trusted third party.

Another technique proposed by [4] secure one way payment system in mobile commerce. This technique uses two modular multiplications, one modular inverse and two hashing by the user using two public key pairs and keyed hash function for computation. In this technique only unilateral communication is sufficient between user and vendor to complete payment. This technique has three main functions; withdrawal, purchase and deposit. Also user does not need to participate in deposit phase so communication load and computation load is low in this scheme. As more than one transaction is involved in this scheme so transaction overhead is present in this scheme.

3. PROPOSED SOLUTION

The proposed framework for the integrity of digitally signed message using joint signature scheme is shown in Fig. 1.

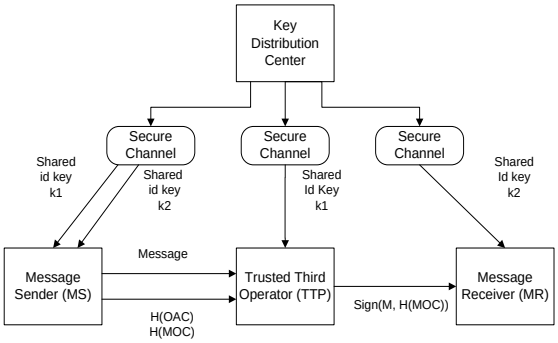

Fig. 1: Proposed Abstract model for message integrity using joint signature scheme

In a proposed model in Fig 1, three main entities are illustrated

- The message sender which is a mobile station (MS).
- The Trusted Third Party which is the network operator used to sign the message in its home environment (TTP).
- And the message receiver which is the service provider that verifies the message and provides different services to the mobile user (MR).

The shared secret keys are securely distributed between these three entities. Message sender sends the encrypted message and H(OAC) and H(MOC) to trusted third party. Trusted third party checks the message integrity with the help of shared key k1 and signs the message with its private key and send to the message receiver which later on verifies the message integrity with secret key k2 and then provide the required service to the message sender.

The notations used in the proposed model are given in table I.

TABLE I. Notations

Notation	Description
MS	Message Sender
TTP	Trusted Third Party
MR	Message Receiver
H (OAC)	Hash of Origin Authentication Code between MS and MR
H (MAC)	Hash of Message Authentication Code between MS and TTP

Journal of Theoretical and Applied Information Technology
20th May 2013. Vol. 51 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Id K1	Secret key shared between MS and TTP
Id K2	Secret key shared between MS and MR

A detailed discussion on integrity of digitally signed message using joint signature scheme is given in the following section.

4. TECHNIQUE

The abstract model of Fig. 1 elaborated by more descriptive model is given below

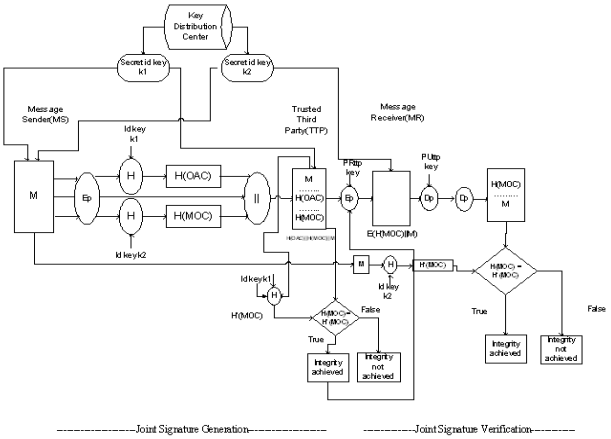

Fig. 2: Cryptographic Model of Message Integrity using joint signature scheme

The above Fig. 2 explains as how message sender MS produces the hash functions and sends it to the trusted third party TTP. Hash function H(OAC) and H(MOC) is produced on key Id K1 and Id K2 respectively, and encrypted message but with different keys securely shared between these three entities. Trusted third party TTP check the integrity of the message by producing its own hash function and comparing it with the received hash from the message sender and then signs the message and produces the joint signature. After verification trusted third party TTP encrypts the message with its private key and sends it to message receiver MR. Message receiver MR decrypts the message with the public key of TTP and produces hash function of its own and then after comparing both hash functions ensures the integrity of the message and provide the required service to the message sender MS.

The process of message integrity using joint signature scheme consist of following four major steps.

Step 1 :(Sharing Secret Key)

The following Fig. 3 shows the distribution of shared secret key K2 between the message sender MS and message receiver MR to verify the integrity of message at Message Receiver side.

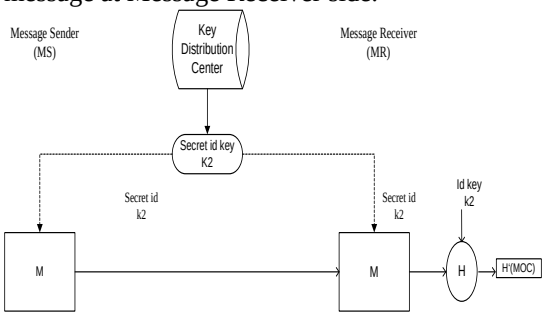

Fig. 3: Distribution of secret keys between (MS) and (MR)

Step 2: (Produce Hash Function)

Message sender MS produces hash funcions H(OAC) and H(MOC) and send it to TTP with the encrypted message. Trusted third party then compare H(MOC) with the H'(MOC) that is produced by TTP on Id key K1 and encrypted message as Id key K1 is shared between MS and TTP. This comparison ensures the integrity of message at the TTP.

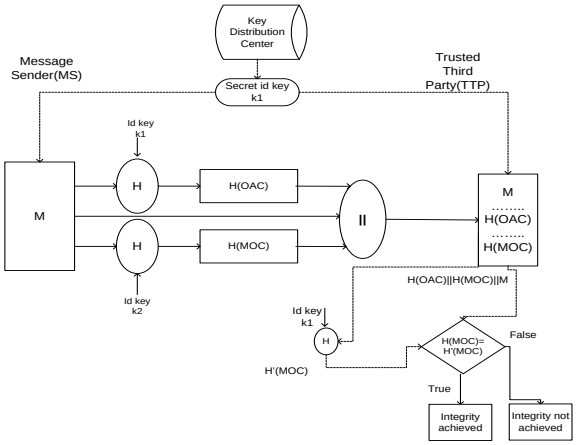

Fig.4 : Message integrity at Trusted Third Party

Step 3: (Joint Signature Generation)

The trusted third party (TTP) signed the message using its private key on Hash Origin Authentication Code H(OAC), a Hash Message Authentication Code H(OMC) and message generated by the MS and sends it to the MR as shown in Fig 5.

Journal of Theoretical and Applied Information Technology
20th May 2013. Vol. 51 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

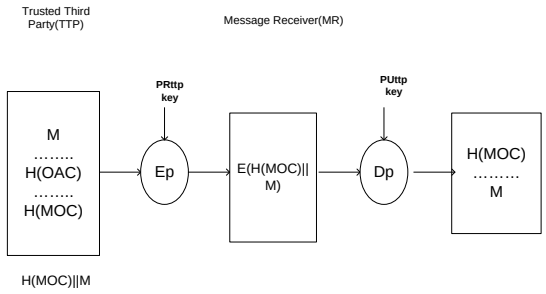

Fig. 5: Joint Signature generation by TTP

Step 4 :(Message Integrity)
The message integrity is verified by the trusted third party (TTP) and by the message receiver (MR) as shown in Fig. 2 and Fig. 3.

5. EXPERIMENTAL RESULTS

Now we will discuss the results in subsections.

A. *Comparison of Different Hash algorithm*

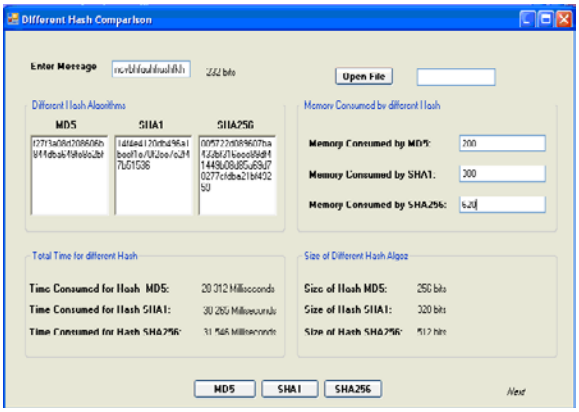

Fig. 6: Different Hash algorithm Comparison

In Fig. 6 MD5, SHA1 and SHA256 are compared with respect to time consuming in calculating hash of message, memory consumed for each hash function, size after calculating hash of message and throughput for each hash algorithm by keeping the actual message size constant and their results are shown in the following Table II.

TABLE II: Comparison Table for Different Hash Algorithm

Hash Algorithm	Message Size	Consumed Memory	Time Consumed for Hashing	Msg Hash Size	Throughput
MD5	384 bits	200 bytes	21.281 msec	256 bits	17 bits/msec
SHA1	384 bits	380 bytes	30.968 msec	320 bits	18 bits/msec
SHA256	384 bits	620 bytes	44.265 msec	512 bits	20 bits/msec

Different graphs obtained from the table values are shown in Fig. 7.

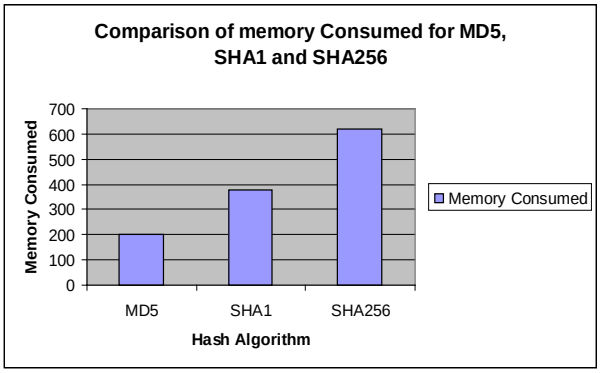

Fig. 7: Memory consumed for different hash algorithm

The figure depicts the total memory consumed for different hash algorithms (MD5, SHA1, and SHA256). The memory is represented in bytes. It is analyzed from the above Fig. 7 that SHA256 consumes more memory than the SHA1 and MD5.

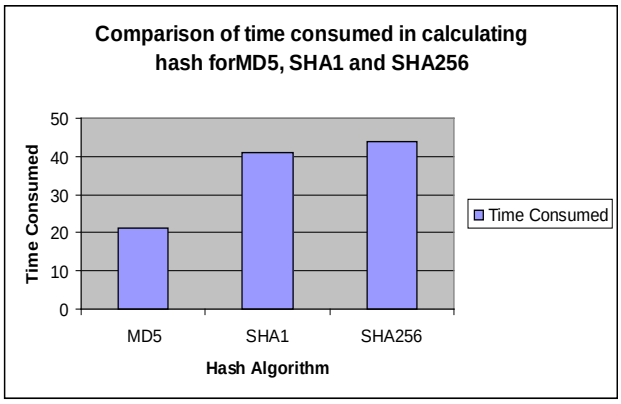

Fig. 8: Time consumed in hash for different hash algorithm

This Fig. 8 shows the time consumed in calculating hash for MD5, SHA1 and SHA256. Time is represented in milliseconds. It is analyzed that SHA256 is slower than the other two algorithms because it takes more rounds to calculate hash than SHA1 which takes five rounds and MD5 that takes four rounds making it more secure than MD5 and SHA1.

Journal of Theoretical and Applied Information Technology
20th May 2013. Vol. 51 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

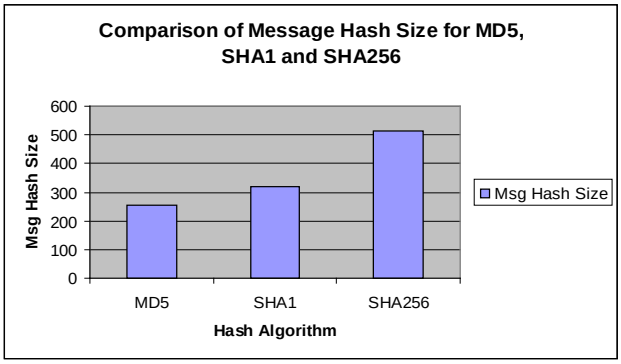

Fig. 9: Message hash size for different hash algorithm

From the Fig. 9 above it is analyzed that the Message hash size for SHA256 is also greater than the Message hash size of MD5 and SHA1 making it more complex to break than the other two.

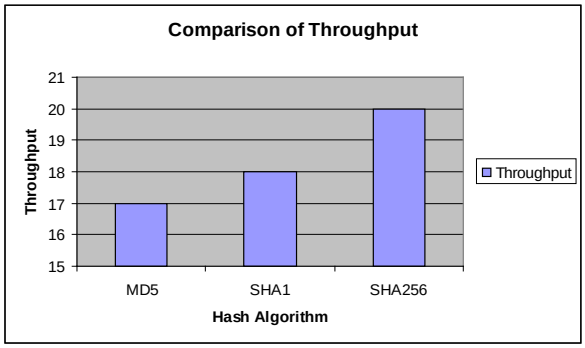

Fig. 10: Throughput for different hash algorithm

Fig. 10 shows the comparison of throughput for MD5, SHA1 and SHA256. Throughput is calculated from the Message hash size and the total time consumed for calculating hash, therefore it is represented in bits per millisecond. SHA256's throughput is greater than MD5 and SHA1 which shows that it is more efficient than the other two w.r.t the message hash size.

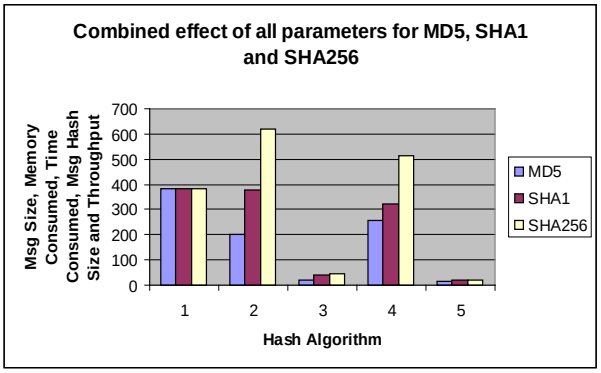

Fig. 11: All parameters for different hash algorithm

Analysis: MD5, SHA1 and SHA256 hashing algorithms are applied to compute hash of the message and analyses the time consumed in computing the hash, memory consumed in computing hash function, throughput and the size of the message after computing hash keeping the actual message size constant. By analyzing the Table II and Fig. 7, 8, 9 10 and 11 it is concluded that SHA256 is more secure than MD5 and SHA1.

B. Comparison of SHA256 for different Message Size

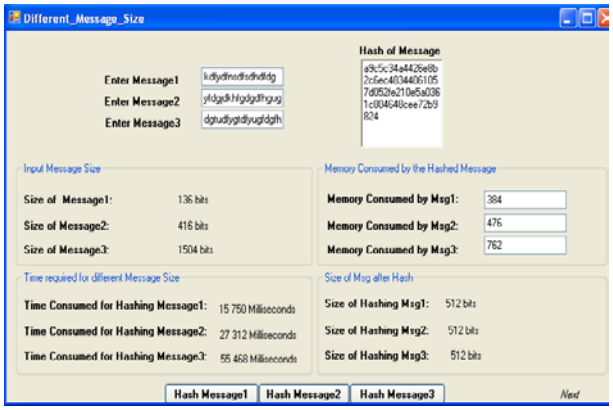

Fig. 12 SHA256 Comparison for different Message Size

In Table III below all the above parameters are calculated for the message having different lengths by my technique SHA256.

TABLE III: Comparison Table for SHA256 for different message size

Hash Algorithm	Message Size	Consumed Memory	Time Consumed for Hashing	Msg Hash Size	Throughput
SHA256	136 bits	384 bytes	15.75 msec	512 bits	8.6 bits/msec
SHA256	416 bits	476 bytes	27.312 msec	512 bits	15.32 bits/msec
SHA256	1504 bits	762 bytes	55.468 msec	512 bits	27.11 bits/msec

Following graphs are plotted from the table values

Journal of Theoretical and Applied Information Technology
20th May 2013. Vol. 51 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

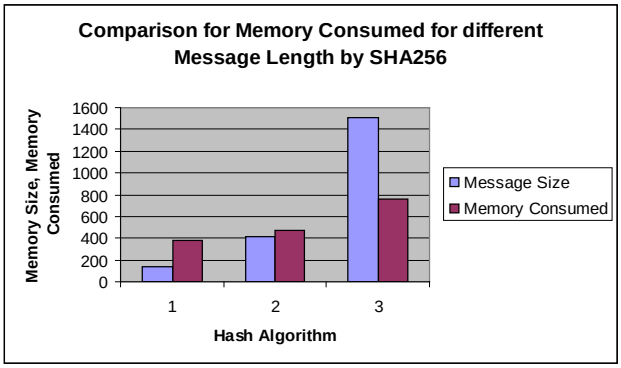

Fig. 13: Memory consumed for different message length

Fig. 13 shows that SHA256 function consume more memory for the calculating hash of greater message length.

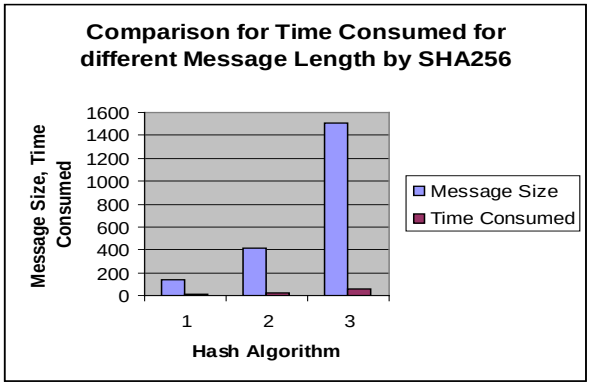

Fig. 14: Time consumed for different message length

The graph depicts in Fig 14 shows that SHA256 require more time to calculate hash of message having the greater length.

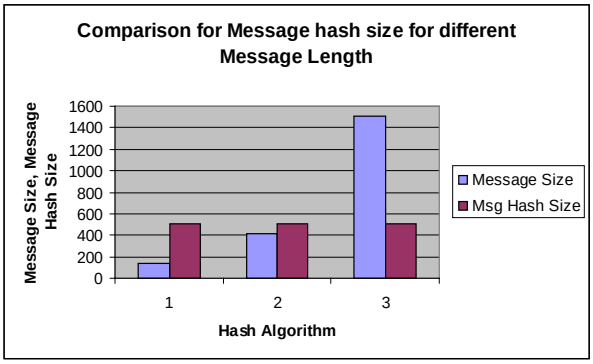

Fig. 15: Message hash size for different message length

It is concluded from the Fig. 15 that message size does not affect the message hash size because it produces the same hash size for any message size.

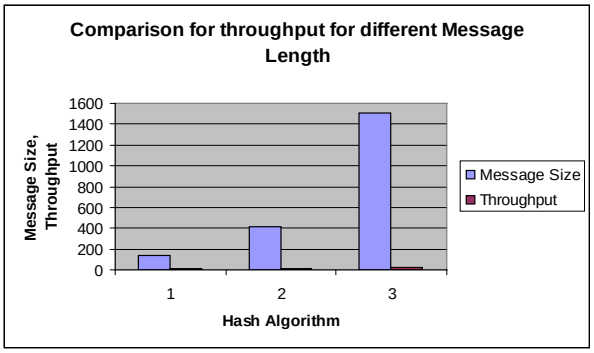

Fig. 16: Throughput for different message length

Fig. 16 concludes that throughput differs a little bit by changing the message size. Here throughput is calculated by the actual message size and the time required for calculating hash.

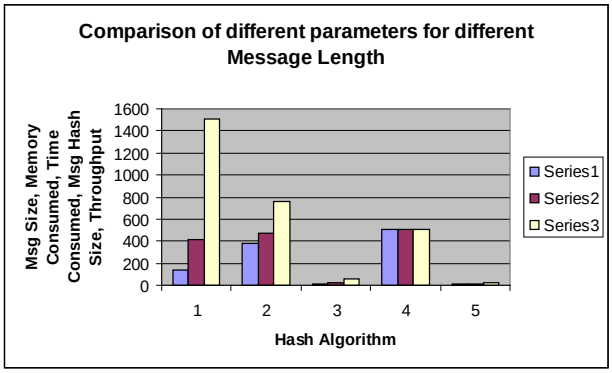

Fig. 17: different parameters for different message length

Analysis: The Fig. 17 above depicts the different message lengths and calculates time consumed in computing the hash, memory consumed, throughput and the size of message after computing hash. From the figure 17 above it is analyzed that the message having more characters take more time for hashing but the size of message after hashing is same for any length ensuring the message hash of any length equally secure.

C. Comparison of Different Encryption\Decryption Algorithm

Journal of Theoretical and Applied Information Technology
20th May 2013. Vol. 51 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

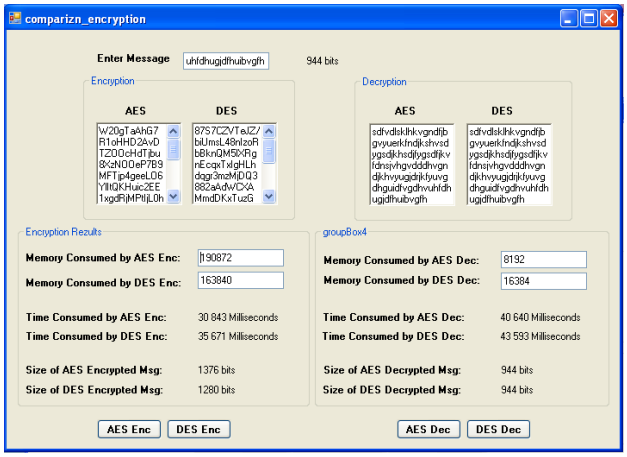

Fig. 18: Different encryption and decryption algorithm Comparison

AES and DES Encryption and Decryption algorithm are compared with respect to consumed memory, time consumed, message size after encryption and throughput. And the values are shown in the following Table IV.

TABLE IV: Comparison Table Encryption Algorithm

Encryption Algorithm	Message Size	Consumed Memory	Time Consumed for Encryption	Encrypted Msg Size	Throughput
AES	944 bits	19872 bytes	30.843 msec	1376 bits	44.61 bits/msec
DES	944 bits	16384 bytes	35.671 msec	1280 bits	35.88 bits/msec

The following graphs are plotted from the calculated results

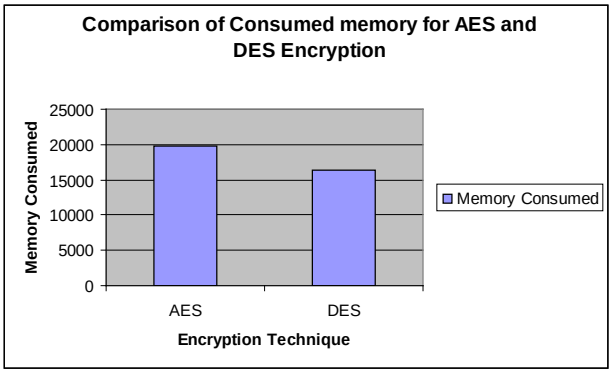

Fig. 19: Memory consumed for AES and DES Encryption

It is observed from fig 19 that AES Encryption function consumes more memory than the DES Encryption showing AES encryption more complex than DES, resulting in requiring greater memory consumption for the decryption algorithm.

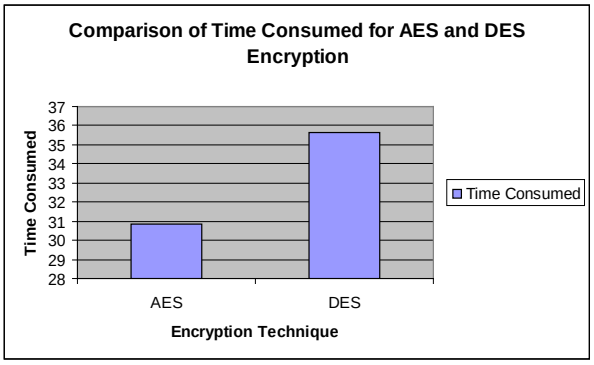

Fig. 20: Time consumed for AES and DES Encryption

AES consume less time than DES Encryption for performing encryption on message which depicts that AES is efficient than DES encryption.

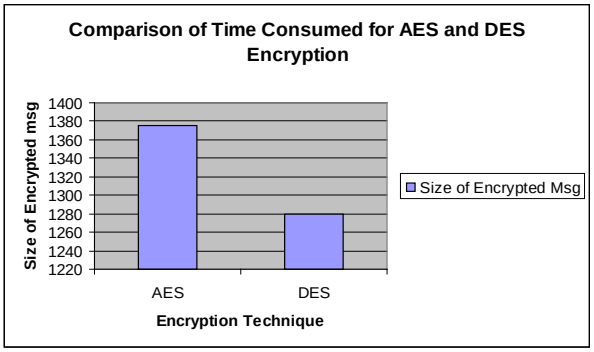

Fig. 21: Consumed message size for AES and DES Encryption

Fig. 21 shows that AES produces greater encrypted message size than produced by the DES encryption algorithm, so AES decryption will require more time to decrypt the message.

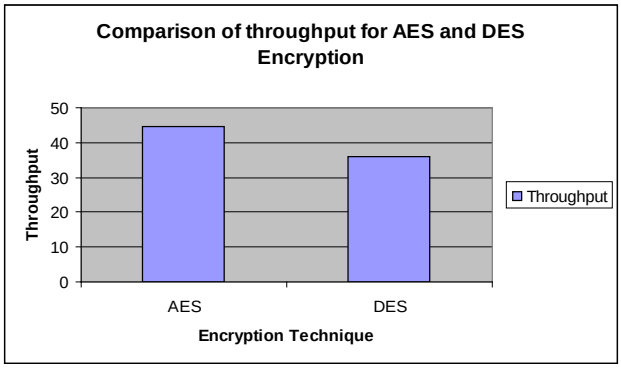

Fig. 22: Throughput for AES and DES Encryption

As AES encrypted message size is greater than DES encrypted message and the time consumed in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

encryption function is less so its throughput is also greater than the DES encryption function. Therefore AES is more secure and efficient technique than DES for encrypting message.

Similarly AES and DES decryption algorithm are also compared for the above mentioned parameters and the results are shown in the following Table V.

TABLE V: Comparison Table Decryption Algorithm

Decryption Algorithm	Consumed Memory	Time Consumed for Decryption	Encrypted Msg Size	Throughput
AES	8192 bytes	43.64 msec	944 bits	21.22 bits/msec
DES	6384 bytes	40.394 msec	944 bits	23.75 bits/msec

Form these calculations following graph is plotted for AES and DES decryption algorithm.

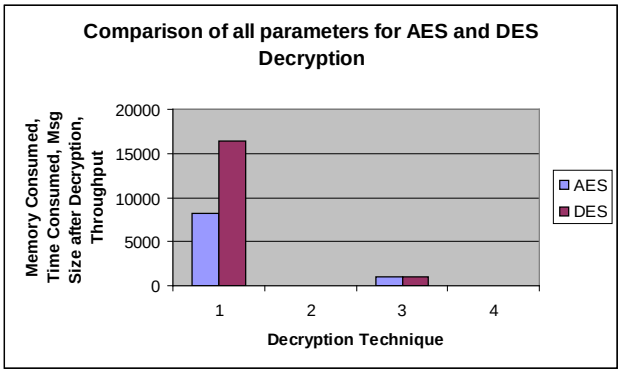

Fig. 23: All parameters for AES and DES decryption

From the Table V and Fig. 23 it is analyzed that AES decryption is more complex than the DES decryption as it requires more memory and time to decrypt the message. So this proves that AES is more secure and complex than DES algorithm.

6. CONCLUSION AND FUTURE WORK

In this paper, we have presented a novel joint signature scheme for ensuring the message integrity that is digitally signed by the mobile user (message sender) with the help of its network operator (trusted third party), both jointly produce the signature which is going to be verified by the vendor (message receiver). Integrity is done on both entities i.e. trusted third party and message receiver which proved them that the message has not been altered by the unauthorized person and delivered as it was sent by the message sender. This scheme involves hash function and encryption/decryption techniques for ensuring message integrity. Furthermore this technique is more efficient and has fewer drawbacks than other traditional schemes which are used for providing security in mobile commerce. In comparison with existing techniques mainly server aided scheme and secure one way mobile payment mechanism, this technique overcomes all the drawbacks of these existing techniques.

In future, I would like to extend joint signature scheme for the message integrity that is digitally signed by the user in order to avoid any fraud over the transmission line. Furthermore this technique can be implemented for other security issues like non-repudiation, confidentiality etc.

REFERENCES

[1] L-S. He And, N. Zhang, "A New Signature Scheme: Joint-Signature," *Proceedings Of The 2004 ACM Symposium On Applied Computing*, Pp 807-812, March 14-17, 2004, Nicosia, Cyprus

[2] J. E. Rice And Y. Zhu, 'A Proposed Architecture For Secure Two-Party Mobile Payment'. *Proceeding Of The IEEE Pacific Rim Conference On Communication, Computer And Digital Processing, 2009*, 23-26 August 2009 Victoria, BC, USA.. Pp 88-93.

[3] C-L. Chen, C-C. Chen, L-C. Liu And G.Horng. 'A Server-Aided Signature Scheme For Mobile Commerce', *Proceeding: IWCMC'07 Proceeding Of The 2007 International Conference On Wireless, Communications And Mobil Computing.* Pp 565-570, 2007.

[4] W. Ham, H. Choi, Y. Xie, M. Lee And K.Kim. 'Secure One-Way Mobile Payment System Keeping Low Computation In Mobile Devices', *Proceeding Of WISA 2002, August 28-30, 2002, Jeju Shilla Hotel*, Pp 287-301,

[5] *W. Diffie, M.E. Hellman. "New Direction In Cryptography".IEEE Transaction On Information Theory, 1976, Vol 22, No. 6, Pp 644-654.*